



Sextortion Scams Become More Threatening in 2025

2025-03-25

U.S. Threats Up 137% Fueled by AI-Powered Attacks and Data Breaches

TEMPE, Ariz. and PRAGUE, March 25, 2025 /PRNewswire/ -- Sextortion scams are becoming more common – and more threatening – as cybercriminals exploit artificial intelligence (AI) and large-scale data breaches to develop highly convincing and personalized scams. A recent analysis by Avast, a leader in digital security and privacy and part of Gen (NASDAQ: GEN), found that in 2025 so far, the risk of being targeted with sextortion scams in the U.S. has risen 137%.

"Sextortion victims frequently receive threatening messages claiming access to their private videos and images. These scams are made even more convincing with the use of stolen passwords from past data breaches, lending an alarming sense of credibility," said Michal Salat, Threat Intelligence Director for Avast. "Fear of exposure, especially when personal details appear accurate, often pressures victims into complying with ransom demands. However, we strongly advise against engaging with these scammers, no matter how real the threats may seem."

New Threatening and Intrusive Tactics

Criminals are refining their tactics, thanks to the help of AI and a wealth of personal data available from recent large-scale breaches. As the sophistication of AI increases, so do the explicit extortion emails, texts and calls from scammers. AI is being used by scammers to create 'deepfake' images, fake explicit photos created by superimposing a victim's face onto another body, coupled with threatening messages to distribute them.

One of the latest techniques used by cybercriminals leverages Google Maps to create a more invasive and personal approach that can really shock and intimidate a victim into complying with their demands.

Criminals – utilizing names, addresses, and emails readily available on the Dark Web due to data breaches – can create very targeted emails to victims containing fabricated footage and unsettling information and images of their real homes. Scammers will also claim to have gained access to victims' devices to extort their victims by threatening to share sexual content or information about them. Cybersecurity experts at Avast have identified over 15,000 unique Bitcoin wallets associated with the Google Maps scams, though the scope of the operation is likely much larger.

Avast experts emphasize the importance of proactive protection against sextortion scams and urge people to never engage with messages that could be from scammers. The following actions help to combat sextortion efforts:

- Do not pay ransom demands or respond to threats.
- Do not engage with these emails, texts or calls or open any associated PDF attachments.
- Always report such crimes to the relevant cybercrime units. In the US victims can reach out to the [FBI](#) or the [Internet Crime Complaint Center](#) (IC3)

- Use a reputable password manager to ensure unique passwords for all accounts and prevent reuse.
- Enable multi-factor authentication (MFA) wherever possible to enhance account security.
- Monitor your data for breaches by using dark web monitoring services, through products such as [Avast Secure Identity](#), to be alerted when personal information is exposed so you can act quickly to help protect your accounts.
- Do not panic - stay informed and take action to secure your accounts.

As sextortion scams become more advanced, it is crucial for individuals to remain cautious and take steps to safeguard their digital privacy. Public awareness and vigilance remain critical in combatting these threats.

For more information, visit <https://www.avast.com/index#pc>.

About Avast

[Avast](#) is a leader in digital security and privacy, and part of Gen™ (NASDAQ: GEN), a global company dedicated to powering Digital Freedom with a family of trusted consumer brands. Avast protects hundreds of millions of users from online threats, for Mobile, PC or Mac, and is top-ranked and certified by VB100, AV-Comparatives, AV-Test, SE Labs and others. Avast is a member of the Coalition Against Stalkerware, No More Ransom and Internet Watch Foundation. Learn more at [Avast.com](#).

Brittney Posey
Gen
press@GenDigital.com

Courtney Rowles
Edelman for Gen
Courtney.Rowles@edelman.com

View original content to download multimedia: <https://www.prnewswire.com/news-releases/sextortion-scams-become-more-threatening-in-2025-302409992.html>

SOURCE Gen Digital Inc.